

4

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月25日
Date of Application:

出願番号 特願2002-341222
Application Number:

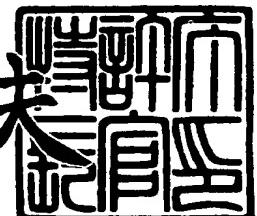
[ST. 10/C] : [JP2002-341222]

出願人 株式会社リコー
Applicant(s):

2003年 7月18日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願
【整理番号】 0206285
【提出日】 平成14年11月25日
【あて先】 特許庁長官 太田 信一郎 殿
【国際特許分類】 G06F 13/00
H04N 1/44
【発明の名称】 ドキュメントセキュリティプロファイル方法、及びその方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラム
【請求項の数】 24
【発明者】
【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
【氏名】 斎藤 敦久
【特許出願人】
【識別番号】 000006747
【氏名又は名称】 株式会社リコー
【代理人】
【識別番号】 100070150
【弁理士】
【氏名又は名称】 伊東 忠彦
【手数料の表示】
【予納台帳番号】 002989
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【フルーフの要否】 要

【書類名】 明細書

【発明の名称】 ドキュメントセキュリティプロファイル方法、及びその方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバープログラム

【特許請求の範囲】

【請求項1】 入出力装置との文書のセキュリティに関する情報の送受信を制御するドキュメントセキュリティプロファイル方法であって、

第1の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、上記文書のコンテンツに埋め込まれる埋め込み情報を上記第1の入出力装置に送信する第1送受信手順と、

第2の入出力装置から受信した上記埋め込み情報に基づいて、上記文書属性情報を上記第2の入出力装置に送信する第2送受信手順とを有することを特徴とするドキュメントセキュリティプロファイル方法。

【請求項2】 上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報とを文書情報として管理する文書情報管理手順を有し、

上記第1送受信手順は、上記文書情報に基づいて上記埋め込み情報を上記第1の入出力装置に送信し、

上記第2送受信手順は、上記文書情報に基づいて上記文書属性情報を上記第2の入出力装置に送信することを特徴とする請求項1記載のドキュメントセキュリティプロファイル方法。

【請求項3】 上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることを特徴とする請求項1又は2記載のドキュメントセキュリティプロファイル方法。

【請求項4】 文書のコンテンツ情報を入出力する入出力装置であって、上記文書を処理する文書処理手段から上記文書のコンテンツ情報を出力を指示する指示情報を受信する指示情報受信手段と、

上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手段と、

上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情



報を取得する取得手段と、

上記埋め込み情報と共に上記文書のコンテンツ情報を出力する出力手段とを有することを特徴とする入出力装置。

【請求項5】 上記取得手段は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手段とを有することを特徴とする請求項4記載の入出力装置。

【請求項6】 上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることを特徴とする請求項4又は5記載の入出力装置。

【請求項7】 文書のコンテンツ情報を入出力する入出力装置であって、上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る讀取手段と、

上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手段と

、
上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手段と、

上記文書属性情報に基づいて上記文書に関する処理を制御する制御手段とを有することを特徴とする入出力装置。

【請求項8】 上記取得手段は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信する受信手段とを有することを特徴とする請求項7記載の入出力装置。

【請求項9】 上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報を文書情報として管理する文書情報管理手段を有することを特徴とする請求項7記載の入出力装置。

【請求項10】 上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることを特徴と

する請求項7乃至9いずれか一項記載の入出力装置。

【請求項11】 文書のセキュリティに関する情報の送受信を行う入出力装置アダプタであって、

上記文書を処理する文書処理手段から上記文書のコンテンツ情報の出力を指示する指示情報を受信する指示情報受信手段と、

上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手段と、

上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情報を取得する取得手段と、

上記埋め込み情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する埋め込み情報送信手段とを有することを特徴とする入出力装置アダプタ。

【請求項12】 上記取得手段は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手段とを有することを特徴とする請求項11記載の入出力装置アダプタ。

【請求項13】 文書のセキュリティに関する情報の送受信を行う入出力装置ドライバプログラムであって、

上記文書を処理する文書処理手段から上記文書のコンテンツ情報の出力を指示する指示情報を受信する指示情報受信手順と、

上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手順と、

上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情報を取得する取得手順と、

上記埋め込み情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する埋め込み情報送信手順とを有することを特徴とする入出力装置ドライバプログラム。

【請求項14】 上記取得手順は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手順と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手順とを有することを特徴とする請求項13記載の入出力装置ドライバプログラム。

【請求項15】 文書のセキュリティに関する情報の送受信を行う入出力装置アダプタであって、

上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手段と、

上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手段と、

上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手段と、

上記文書属性情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する文書属性情報送信手段とを有することを特徴とする入出力装置アダプタ。

【請求項16】 上記取得手段は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信する受信手段とを有することを特徴とする請求項15記載の入出力装置アダプタ。

【請求項17】 文書のセキュリティに関する情報の送受信を行う入出力装置ドライバプログラムであって、

上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手順と、

上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手順と、

上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手順と、

上記文書属性情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する文書属性情報送信手順とを有することを特徴とする入出力装置ドライバプログラム。

【請求項18】 上記取得手順は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手順と、

上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信する受信手順とを有することを特徴とする請求項17記載の入出力装置ドライバプログラム。

【請求項19】 文書を処理する文書処理手段との間で該文書のセキュリティに関する情報が格納された文書ファイルの送受信を制御するドキュメントセキュリティプロファイル方法であって、

第1の文書処理手段から上記文書ファイルを受信する第1の受信手順と、
上記文書に関する処理の要件を有するセキュリティポリシーに基づいて、上記文書ファイルに対応する上記文書のセキュリティに関する文書属性情報を付加して上記第1の文書処理手段に送信する第1の送信手順とを有することを特徴とするドキュメントセキュリティプロファイル方法。

【請求項20】 第2の文書処理手段から上記文書に関する処理を行うユーザーを識別するユーザー属性情報を受信する第2の受信手順と、

上記ユーザー属性情報に基づいて、上記文書の処理の可否を上記第2の文書処理手段に送信する第2の送信手順とを有することを特徴とする請求項19記載のドキュメントセキュリティプロファイル方法。

【請求項21】 上記第1の送信手順は、上記文書ファイルに、上記文書属性情報、上記ユーザー属性情報、及び上記文書に関する処理を許可する要件、上記文書に関する処理を禁止する要件、上記セキュリティポリシーのうち少なくとも一つを附加して上記第1の入出力装置に送信することを特徴とする請求項19又は20記載のドキュメントセキュリティプロファイル方法。

【請求項22】 文書のセキュリティに関する情報が格納された文書ファイルの配布を行うドキュメントセキュリティプロファイル方法であって、

上記文書ファイルを上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する第1の送信手順と、

上記管理手段から上記文書に関する処理の要件が付加された文書ファイルを受信する第1の受信手順と、

上記文書に関する処理の要件が付加された文書ファイルを上記文書を処理する他の文書処理手段に送信する文書ファイル送信手順とを有することを特徴とするドキュメントセキュリティプロファイル方法。

【請求項23】 上記文書に関する処理の要件が付加された文書ファイルを受信する第2の受信手順と、

上記文書に関する処理の要件及び上記文書に関する処理結果に基づいて、上記文書に関する処理を行うユーザーを識別する識別手順と、

上記識別手順の識別結果を示すユーザー属性情報に対応する上記文書の処理の可否を取得する取得手順と、

上記ユーザー属性情報及び上記文書の処理の可否に基づいて、上記文書のコンテンツ情報を入出力する入出力手段を制御する制御手順とを有することを特徴とする請求項22記載のドキュメントセキュリティプロファイル方法。

【請求項24】 上記第1の受信手順は、上記文書ファイルに、上記文書属性情報、上記ユーザー属性情報、及び上記文書に関する処理を許可する要件、上記文書に関する処理を禁止する要件、上記セキュリティポリシーのうち少なくとも一つを付加することを特徴とする請求項22又は23記載のドキュメントセキュリティプロファイル方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ドキュメントセキュリティプロファイル方法に係り、特に、ドキュメント（文書）に関するセキュリティ情報を送受信するドキュメントセキュリティプロファイル方法に関する。

【0002】

また、本発明は、そのようなドキュメントセキュリティプロファイル方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラムに関する。

【0003】

【従来の技術】

近年、多くのオフィス業務では、プリンタ、複合機などの入出力装置を用いて文書が扱われている。このような入出力装置に依存して日常の業務が行われるにつれて、その文書を扱う入出力装置のセキュリティ確保が重要視されるようになってきている。特に、最近では官公庁を中心としてISO17799として知られる情報セキュリティ管理標準に基づいて組織の情報セキュリティを掲げるところが増え、そのポリシーに基づいてセキュリティを確保した入出力装置に関するシステムの構築・運営が行われている。このような動向は、官公庁から自治体、そして取引先である大手企業に広がる傾向にあり、大手企業の取引先である中小企業へとその動きが広がっていくことが容易に予想できる。この動向そのものは、健全な入出力装置システムの構築を加速させるものとして歓迎すべきである。

【0004】

また、上記のような入出力装置システムに設定するセキュリティ情報（通常ポリシーファイルという形式で設定される）には、例えば、Java（登録商標）に設定するプログラムの実行許諾に関する設定情報や、ファイアウォールに設定するプロトコルの通過許可に関する設定情報などがある。

【0005】

一般に、入出力装置システムのセキュリティの確保は、機密性、完全性、可用性の確保に大別される。完全性や可用性は入出力装置システムの管理者が適切に運営・管理すれば、実質上問題のないレベルを確保できる場合が多い。一方、機密性の確保のためには、中小企業に代表される入出力装置のユーザー組織に所属するユーザーのそれぞれにセキュリティポリシーを共有・徹底させなければならない。このような理由で、特に、入出力装置のコンテナである文書に対するポリシー、中でも機密保持に関するポリシーが重要視されているため、多くの企業では、文書に関するセキュリティを制御する要求が高まっている。

【0006】

例えば、従来技術として、識別情報を付加して印刷処理を行い、他の機器からの識別情報の問い合わせに答える文書管理装置と他の機器が接続された文書管理システムでは、プリンタで出力するときは良いが、他の機器でその文書が取り扱われるときに、文書管理システム全体が機能している必要がある。また、他の機

①

器で必要となる情報が大きくなない場合でも、文書管理システム全体で管理している大きな情報を検索する必要もある（例えば、特許文献1参照）。

【0007】

また、従来技術として、特開平7-154617号（特許文献8参照）の機密文書を識別して、コピーを停止する、コピー時の情報を同時に印字する方法と、特開平7-154617号（特許文献8参照）の機密認識マークを検知して複写動作の制御を行う方法では、紙文書の特定のパターンや機密認識マークなどの情報を複写機内部に登録しておくため、それらの情報に柔軟性がなく、それに付随する動作にも柔軟性がない（例えば、特許文献2参照）。

【0008】

また、従来技術として、画像から特定の記号を取り出し、認識する方法では、画像への出力方法まで言及されていないため、紙の出力と入力、電子ファイルの出力と入力などの連携をとることはできない（例えば、特許文献3参照）。

【0009】

また、従来技術として、ユーザーの識別情報に関連した印刷、複写の制御はいくつか出されているが、文書の識別情報を印刷し、複写、配布し、読み出しなどの一連の動作で扱うような出願は見られない（例えば、特許文献4参照）。

【0010】

【特許文献1】

特開2000-261584号公報

【特許文献2】

特許第3203103号明細書

【特許文献3】

特開平7-66970号公報

【特許文献4】

特開2001-125759号公報

【特許文献5】

特開2002-197101号公報

【特許文献6】

特開2002-197101号公報

【特許文献7】

特開平7-58950号公報

【特許文献8】

特開平7-154617号公報

【0011】

【発明が解決しようとする課題】

上記のように現在、多くの企業ではセキュリティ情報を設定し、そのセキュリティを制御しようとしているが、実際、オフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、また、オフィスシステムを構成するさまざまな入出力装置に関して、個別にセキュリティ設定を行う必要がある。従って、このようなセキュリティ設定を行うためにさまざまな入出力装置に関する知識が必要となってしまうという問題点があった。

【0012】

また、複数の入出力装置の一つ一つにセキュリティ情報を設定しなければならならず、手間が煩雑になるという問題点があった。

【0013】

このように従来の複数の入出力装置では個別にセキュリティ設定を行っているため、入出力装置システム全体がどのようなセキュリティ状態になっているかを把握するのが難しいという問題点があった。

【0014】

そこで、本発明の課題は、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができるドキュメントセキュリティプロファイル方法、及びその方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラムを提供することである。

【0015】

【課題を解決するための手段】

上記の課題を解決するため、本発明は、入出力装置との文書のセキュリティに

関する情報の送受信を制御するドキュメントセキュリティプロファイル方法であって、第1の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、上記文書のコンテンツに埋め込まれる埋め込み情報を上記第1の入出力装置に送信する第1送受信手順と、第2の入出力装置から受信した上記埋め込み情報に基づいて、上記文書属性情報を上記第2の入出力装置に送信する第2送受信手順とを有する構成とされる。

【0016】

このようなドキュメントセキュリティプロファイル方法では、第1の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、文書のコンテンツに埋め込まれる埋め込み情報を第1の入出力装置に送信し、第2の入出力装置から受信した埋め込み情報に基づいて、文書属性情報を第2の入出力装置に送信することにより、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができる。

【0017】

文書のセキュリティに関する情報を管理するという観点から、本発明は、請求項2に記載されるように、上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報を文書情報として管理する文書情報管理手順を有し、上記第1送受信手順は、上記文書情報に基づいて上記埋め込み情報を上記第1の入出力装置に送信し、上記第2送受信手順は、上記文書情報に基づいて上記文書属性情報を上記第2の入出力装置に送信するように構成することができる。

【0018】

このようなドキュメントセキュリティプロファイル方法では、文書を識別する識別情報に対応付けて文書属性情報と埋め込み情報を文書情報として管理し、文書情報に基づいて埋め込み情報を第1の入出力装置に送信し、文書情報に基づいて文書属性情報を第2の入出力装置に送信することにより、効率的に文書情報から文書属性情報や埋め込み情報を参照して入出力装置に送信することができる。

【0019】

文書のコンテンツへ埋め込まれる埋め込み情報を様々な情報で適応させるという観点から、本発明は、請求項3に記載されるように、上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であるように構成することができる。

【0020】

このようなドキュメントセキュリティプロファイル方法では、埋め込み情報が文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることにより、埋め込み情報で文書のコンテンツや文書属性を識別することができる。

【0021】

埋め込み情報と共に文書のコンテンツ情報を出力するという観点から、本発明は、請求項4に記載されるように、文書のコンテンツ情報を入出力する入出力装置であって、上記文書を処理する文書処理手段から上記文書のコンテンツ情報を出力を指示する指示情報を受信する指示情報受信手段と、上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手段と、上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情報を取得する取得手段と、上記埋め込み情報と共に上記文書のコンテンツ情報を出力する出力手段とを有する構成とすることができる。

【0022】

このような入出力装置では、文書を処理する文書処理手段から文書のコンテンツ情報を出力を指示する指示情報を受信し、指示情報に基づいて文書のセキュリティに関する文書属性情報を抽出し、文書属性情報に対応する文書のコンテンツに埋め込まれる埋め込み情報を取得し、埋め込み情報と共に文書のコンテンツ情報を出力することにより、文書に関するセキュリティ情報を取得して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【0023】

文書属性情報に対応する埋め込み情報を受信するという観点から、本発明は、請求項5に記載されるように、上記取得手段は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、



上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手段とを有するように構成することができる。

【0024】

このような入出力装置では、文書属性情報を文書のセキュリティに関するプロファイルを管理する管理手段に送信し、管理手段から送信された文書属性情報に対応する埋め込み情報を受信することにより、文書に関するセキュリティ情報を送受信して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【0025】

文書属性情報に基づいて文書に関する処理を制御するという観点から、本発明は、請求項7に記載されるように、文書のコンテンツ情報を入出力する入出力装置であって、上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手段と、上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手段と、上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手段と、上記文書属性情報に基づいて上記文書に関する処理を制御する制御手段とを有するように構成することができる。

【0026】

このような入出力装置では、上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取り、文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出し、埋め込み情報に対応する文書のセキュリティに関する文書属性情報を取得し、文書属性情報に基づいて文書に関する処理を制御することにより、文書に関するセキュリティ情報を取得して、そのセキュリティを反映させた文書に関する処理を制御することができる。

【0027】

埋め込み情報に対応する文書属性情報を受信するという観点から、本発明は、請求項8に記載されるように、上記取得手段は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリテ

イに関する文書属性情報を受信する受信手段とを有するように構成することができる。

【0028】

このような入出力装置では、埋め込み情報を文書のセキュリティに関するプロファイルを管理する管理手段に送信し、管理手段から送信された埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信することにより、文書に関するセキュリティ情報を送受信して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【0029】

文書のセキュリティに関する情報を管理するという観点から、本発明は、請求項9に記載されるように、上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報を文書情報として管理する文書情報管理手段を有するように構成することができる。

【0030】

このような入出力装置では、文書を識別する識別情報に対応付けて文書属性情報と埋め込み情報を文書情報として管理することにより、効率的に文書属性情報を取得して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【0031】

セキュリティポリシーに基づいた情報を附加した文書ファイルを送受信するという観点から、本発明は、請求項19に記載されるように、文書を処理する文書処理手段との間で該文書のセキュリティに関する情報が格納された文書ファイルの送受信を制御するドキュメントセキュリティプロファイル方法であって、第1の文書処理手段から上記文書ファイルを受信する第1の受信手順と、上記文書に関する処理の要件を有するセキュリティポリシーに基づいて、上記文書ファイルに対応する上記文書のセキュリティに関する文書属性情報を附加して上記第1の文書処理手段に送信する第1の送信手順とを有するように構成することができる。

【0032】

このようなドキュメントセキュリティプロファイル方法では、第1の文書処理手段から上記文書ファイルを受信し、文書に関する処理の要件を有するセキュリティポリシーに基づいて、文書ファイルに対応する文書のセキュリティに関する文書属性情報を附加して第1の文書処理手段に送信することにより、文書を処理する文書処理手段との間でセキュリティを反映させた文書ファイルの送受信を制御することができる。

【0033】

セキュリティポリシーに基づいた情報を附加した文書ファイルを送受信するという観点から、本発明は、請求項20に記載されるように、第2の文書処理手段から上記文書に関する処理を行うユーザーを識別するユーザー属性情報を受信する第2の受信手順と、上記ユーザー属性情報に基づいて、上記文書の処理の可否を上記第2の文書処理手段に送信する第2の送信手順とを有するように構成することができる。

【0034】

このようなドキュメントセキュリティプロファイル方法では、第2の文書処理手段から文書に関する処理を行うユーザーを識別するユーザー属性情報を受信する第2の受信手順と、ユーザー属性情報に基づいて、文書の処理の可否を第2の文書処理手段に送信することにより、セキュリティポリシーに基づいて複数の文書処理手段での処理を制御することができる。

【0035】

文書のセキュリティに関する情報に柔軟性を持たせるという観点から、本発明は、請求項21に記載されるように、上記第1の送信手順は、上記文書ファイルに、上記文書属性情報、上記ユーザー属性情報、及び上記文書に関する処理を許可する要件、上記文書に関する処理を禁止する要件、上記セキュリティポリシーのうち少なくとも一つを附加して上記第1の入出力装置に送信するように構成することができる。

【0036】

このようなドキュメントセキュリティプロファイル方法では、文書ファイルに、文書属性情報、ユーザー属性情報、文書に関する処理を許可する要件、文書に

関する処理を禁止する要件、セキュリティポリシーのうち少なくとも一つを付加することにより、効率的に複数の文書処理手段での処理を制御することができる。

【0037】

文書処理手段により文書のセキュリティに関する情報が格納された文書ファイルの配布を行うという観点から、本発明は、請求項22に記載されるように、文書のセキュリティに関する情報が格納された文書ファイルの配布を行うドキュメントセキュリティプロファイル方法であって、上記文書ファイルを上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する第1の送信手順と、上記管理手段から上記文書に関する処理の要件が付加された文書ファイルを受信する第1の受信手順と、上記文書に関する処理の要件が付加された文書ファイルを上記文書を処理する他の文書処理手段に送信する文書ファイル送信手順とを有するように構成することができる。

【0038】

このようなドキュメントセキュリティプロファイル方法では、文書ファイルを文書のセキュリティに関するプロファイルを管理する管理手段に送信し、管理手段から上記文書に関する処理の要件が付加された文書ファイルを受信し、文書に関する処理の要件が付加された文書ファイルを、その文書を処理する他の文書処理手段に送信することにより、文書処理手段により文書のセキュリティに関する情報が付加された文書ファイルを受信し、受信した文書ファイルを他の文書処理手段に配布することができる。

【0039】

セキュリティポリシーに基づいた情報を付加した文書ファイルを送受信するという観点から、本発明は、請求項23に記載されるように、上記文書に関する処理の要件が付加された文書ファイルを受信する第2の受信手順と、上記文書に関する処理の要件及び上記文書に関する処理結果に基づいて、上記文書に関する処理を行うユーザーを識別する識別手順と、上記識別手順の識別結果を示すユーザー属性情報に対応する上記文書の処理の可否を取得する取得手順と、上記ユーザー属性情報及び上記文書の処理の可否に基づいて、上記文書の処理を行う処理手

順とを有するように構成することができる。

【0040】

このようなドキュメントセキュリティプロファイル方法では、文書に関する処理の要件が付加された文書ファイルを受信し、文書に関する処理の要件及び文書に関する処理結果に基づいて、文書に関する処理を行うユーザーを識別し、識別手順の識別結果を示すユーザー属性情報に対応する文書の処理の可否を取得し、ユーザー属性情報及び文書の処理の可否に基づいて、文書のコンテンツ情報を入出力する入出力手段を制御することにより、配布された文書ファイルに基づいて、効率的に入出力手段の処理を制御することができる。

【0041】

また、上記課題を解決するため、本発明は、上記ドキュメントセキュリティプロファイル方法における処理を行う入出力装置アダプタ、入出力装置ドライバプログラムとすることもできる。

【0042】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。本発明の実施の一形態に係るドキュメントセキュリティプロファイル方法は、プリンタや複合機などの入出力装置へ文書属性情報や埋め込み情報を送受信する。その入出力装置のハードウェア構成は、例えば、図1に示すようになっている。尚、上記プロファイルとは、文書のセキュリティに関する情報を示している。

【0043】

図1は、本発明の第1実施例に係る入出力装置のハードウェア構成を示すブロック図である。

【0044】

図1において、入出力装置10は、CPU11と、ROM12と、RAM13と、HDD14と、スキャナ15と、プロッタ16と、表示操作部17と、NIC (Network Interface Card) 18とで構成される。これらの各ユニットはバス19を介して接続されている。CPU11は、ROM12に格納された入出力装置を制御するためのプログラム（ドライバプログラム）

、及びHDD14からRAM13に転送されるプログラムとに基づいて、入出力装置10を制御する。また、CPU11は、RAM13を作業メモリ空間として利用すると共に、RAM13から処理対象のデータを読み出して処理する。処理後のデータはRAM13に格納される。HDD14は、文書ファイル、ドキュメントセキュリティプロファイル方法に係るプログラムなどを格納する。スキャナ15は、印刷物をスキャンして電子データとして取り込むスキャナ処理を行う。プロッタ16は、パソコンコンピュータ（PC）などで生成した電子文書を印刷する場合や、印刷物などを複写する印刷処理を行う。NIC18は、ネットワークインターフェースであり、ネットワークと接続されて複数の入出力装置とドキュメントセキュリティプロファイル方法に関する文書属性、埋め込み情報などの送受信を行う。表示操作部17は、オペレーションパネルなどで構成され、ユーザーからの入力操作の受け付け並びにユーザーに向けた表示を行う。

【0045】

このようなハードウェア構成を採用することにより、複数の入出力装置10のセキュリティを統括して管理し、そのセキュリティを反映させた印刷処理などを行うことができる。

【0046】

次に、第1実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図2は、本発明の第1実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図2において、ドキュメントセキュリティシステム2は、文書に関する処理を制御する文書処理部20と、ドキュメントセキュリティプロファイル方法における処理が行われるドキュメントセキュリティプロファイル処理部30と、図2に示す入力装置10の構成を有するプリンタ40、複合機50とで構成される。尚、文書処理部20と、ドキュメントセキュリティプロファイル処理部30と、プリンタ40と、複合機50は、LANなどのネットワーク1を介して接続されている。尚、文書処理部20と、ドキュメントセキュリティプロファイル処理部30は、それぞれ別のサーバに設置するようにしてもよいし、一つのサーバに設置するようにしてもよい。

【0047】

文書処理部20は、プリンタ40に文書のプリントを指示する情報を送信する。ドキュメントセキュリティプロファイル処理部30は、プリンタ40及び複合機50へ文書に関するセキュリティ情報を送受信する。プリンタ40は、例えば、文書情報及び文書に関するセキュリティ情報を紙へプリントする出力処理を行う。複合機50は、例えば、紙にプリントされた文書情報及び文書に関するセキュリティ情報をスキャンする入力処理を行う。

【0048】

次に、第1実施例におけるドキュメントセキュリティプロファイル処理の手順について説明する。図2に示すように、先ず、ステップS1の処理で、文書処理部20は、プリンタ40に文書のプリントを指示する指示情報を送信する。この指示情報には、プリントする文書情報、文書属性を含んでいる。ステップS2の処理で、プリンタ40は、指示情報から文書属性を抽出し、その文書属性をドキュメントセキュリティプロファイル処理部30に送信する。ステップS3の処理で、ドキュメントセキュリティプロファイル処理部30は、送信された文書属性に基づいて、文書情報への埋め込み情報を作成し、プリンタ40に送信する。ステップS4の処理で、プリンタ40は、受信した埋め込み情報に基づいて、紙60に文書情報と共に埋め込み情報61をプリントする出力処理を行う。

【0049】

ステップS5の処理で、複合機50は、紙60にプリントされた文書情報と共に埋め込み情報61をスキャンする入力処理を行う。ステップS6の処理で、複合機60は、ドキュメントセキュリティプロファイル処理部30にスキャンした埋め込み情報61を送信する。ステップS7の処理で、ドキュメントセキュリティプロファイル処理部30は、埋め込み情報61に基づいて文書属性を取得し、その文書属性を複合機50に送信する。複合機50は、受信した文書属性に基づいてスキャンした文書情報に関する処理を制御する。複合機50の処理について、例えば、複写処理の場合、複写の停止や、「複写禁止」、「社外秘」などのラベルを印字する、ユーザー情報、日時情報を印字する、特殊な紙への複写、複写の履歴情報の格納などの処理を行う。また、複合機50は、スキャンした文書に



関する情報の配信処理の場合、配信の停止、「複写禁止」、「社外秘」などのすかしを追加する、ユーザー情報、日時情報を追加する、特定のフォルダへのコピー配信、配信の履歴情報の格納などの処理を行う。

【0050】

次に、第2実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図3は、本発明の第2実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。尚、図3に示すシステム構成は、図2に示すシステム構成と略同様であるため、同様の構成及び手順については同符号を付し、また、同様の構成のうち一部分の構成を省略する。以下、図5、図6、図8に示すシステム構成についても同様とする。

【0051】

図3において、ドキュメントセキュリティシステム3は、文書属性と埋め込み情報である画像情報とが格納された文書情報DB31を有する構成とされる。ドキュメントセキュリティプロファイル処理部30は、送信された文書属性に基づいて、文書情報DB31に格納された埋め込み情報61をプリンタ40に送信する。プリンタ40は、送信された埋め込み情報61に基づいて、紙60に文書情報に重ねて埋め込み情報61をプリントする。

【0052】

次に、文書情報DB31に格納された文書情報について説明する。図4は、文書情報DBに格納されたテーブルを示す図である。図4において、テーブル310は、文書を識別する文書IDと、文書属性を格納した文書属性ファイルと、埋め込み情報とで構成される。ここで文書IDは、日時やドキュメントセキュリティプロファイル処理部30を識別するIDや、プリンタ40を識別するIDなどの組み合わせ、また、それにシリアル番号などを付加して一意に定まる情報が用いられている。尚、埋め込み情報は、文書を一意に識別するバーコード情報、透かし情報、地紋情報などが適応される。例えば、バーコード情報の場合、文書IDをそのままエンコードしたり、シリアル番号などをエンコードしたりして一意に定まる情報を格納している。尚、テーブル310に格納される情報は、文書の保存期限などが定められている場合、その保存期限内は唯一のIDとなるように

設定する。

【0053】

次に、第3実施例におけるドキュメントセキュリティプロファイル処理部30が複合機51内に設けられた場合のシステム構成について説明する。図5は、本発明の第3実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図5において、ドキュメントセキュリティシステム4は、文書属性と埋め込み情報である画像情報とが格納された文書情報DB31と、ドキュメントセキュリティプロファイル処理部30が設けられた複合機51とを有する構成とされる。このように、複合機51内にドキュメントセキュリティプロファイル処理部30を設置することにより、他のサーバを設置して動作させる必要がないため、システムの簡略化を図ることができる。

【0054】

次に、第4実施例におけるプリンタが除かれた場合のシステム構成について説明する。図6は、本発明の第4実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図6において、ドキュメントセキュリティシステム5は、文書属性と埋め込み情報である画像情報とが格納された文書情報DB31と、プリント機能を有し、ドキュメントセキュリティプロファイル処理部30が設けられた複合機51とを有する構成とされる。先ず、複合機51は、文書処理部20からのプリント指示情報を受信すると、ステップS2の処理で、複合機51のドキュメントセキュリティプロファイル処理部30は、文書情報DB31から文書属性を参照する。また、ステップS3の処理で、ドキュメントセキュリティプロファイル処理部30は、文書情報DB31から埋め込み情報61を受信する。このように、プリンタ40を除き、複合機51内にドキュメントセキュリティプロファイル処理部30を設置することにより、他のサーバを設置して動作させる必要がないため、システムの簡略化を図ることができる。

【0055】

次に、第5実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図7は、本発明の第5実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。尚、図7に示す

システム構成は、図2に示すシステム構成と略同様であるため、同様の構成及び手順については同符号を付して説明を省略する。図7において、ドキュメントセキュリティシステム6は、ドキュメントセキュリティプロファイル処理部30からの文書に関する情報の送受信をプリンタ40、複合機50が対応することができない場合、プリンタ40に接続されたアダプタ70と、複合機50に接続されたアダプタ71とを有する構成とされる。

【0056】

次に、各アダプタ70、71での処理手順を説明する。先ず、ステップS1の処理で、プリンタ40に接続されたアダプタ70は、文書処理部20から文書のプリントを指示する指示情報を受信する。ステップS2の処理で、アダプタ70は、ドキュメントセキュリティプロファイル処理部30へ文書属性を送信する。ステップS3の処理で、アダプタ70は、ドキュメントセキュリティプロファイル処理部30からの埋め込み情報を受信する。ステップS4の処理で、プリンタ40は、アダプタ70から取得した埋め込み情報に基づいて、紙60に文書情報と共に埋め込み情報61をプリントする出力処理を行う。

【0057】

一方、ステップS5の処理で、複合機50は、紙60にプリントされた文書情報と共に埋め込み情報61をスキャンする入力処理を行う。ステップS6の処理で、アダプタ71は、ドキュメントセキュリティプロファイル処理部30へ埋め込み情報を送信する。ステップS7の処理で、アダプタ71は、ドキュメントセキュリティプロファイル処理部30からの文書属性を受信する。複合機50は、受信した文書属性に基づいてスキャンした文書情報に関する処理を制御する。

【0058】

このように、プリンタ40に接続されたアダプタ70と、複合機50に接続されたアダプタ71とを設けることにより、ドキュメントセキュリティプロファイル処理部30からの文書に関する情報の送受信を行うことができる。

【0059】

次に、第6実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図8は、本発明の第6実施例に係るドキュメント



セキュリティプロファイル方法におけるシステム構成図である。図8において、ドキュメントセキュリティシステム7は、文書のプリント指示情報を送信する前に、ドキュメントセキュリティプロファイル処理部30から埋め込み情報を取得する文書処理部20を有する構成とされる。先ず、ステップS1の処理で、文書処理部20は、ドキュメントセキュリティプロファイル処理部30へ文書属性を送信する。ステップS2の処理で、ドキュメントセキュリティプロファイル処理部30は、受信した文書情報に基づいて、文書処理部20へ埋め込み情報を送信する。ステップS3の処理で、文書処理部20は、プリンタ40へ埋め込み情報と共に、効率的にプリントを指示する指示情報を送信する。

【0060】

このように、文書処理部20はプリンタ40へ埋め込み情報と共に、プリントを指示する指示情報を送信することにより、プリンタ40で文書情報のプリントを行う出力処理を効率的に行うことができる。

【0061】

尚、プリンタ40に送信される埋め込み情報に、複合機50を制御する情報を付加するようにしてもよい。これにより、ドキュメントセキュリティプロファイル処理部30が停止している場合、複合機50での処理を制御することができる。例えば、複合機50で「極秘」などの文書属性が抽出された場合、複写処理を停止するなどの基本的な制御情報を付加することができる。

【0062】

尚、プリンタ40又は複合機50で文書に関する入出力処理を行うときに、ドキュメントセキュリティプロファイル処理部30が停止している場合、文書属性を抽出し、即座に動作を停止することなく、最小限の情報で最低限の入出力処理を行う第一の埋め込み情報と、より多くの文書に関する情報を抽出して様々な処理を制御するための第二の埋め込み情報を埋め込むようにしてもよい。

【0063】

次に、電子的な埋め込み情報としてPDF（Portable Document Format）ファイルを用い、ドキュメントセキュリティポリシー（以下総称してDSP（Document Security Policy）と呼

ぶ)に基づいて文書に関する情報を送受信する第7実施例に説明する。

【0064】

先ず、第7実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図9は、本発明の第7実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図9において、ドキュメントセキュリティシステム8は、PDF200を有するドキュメントセキュリティプロファイル処理部32と、文書属性とPDFファイルを送受信する文書処理部21と、ユーザーを認証するプラグインを有する文書処理部22とを有する構成とされる。

【0065】

次に、ドキュメントセキュリティシステム8での処理手順を説明する。先ず、ステップS1の処理で、文書処理部21は、ドキュメントセキュリティプロファイル処理部32に文書属性と、PDFファイル25とを送信する。ステップS2の処理で、ドキュメントセキュリティプロファイル処理部32は、文書情報をPDFファイル25に埋め込み、セキュリティプロテクトされたPDFファイル26を文書処理部21に送信する。ステップS3の処理で、文書処理部21は、受信したセキュリティプロテクトされたPDFファイル26を文書処理部22に配布する。

【0066】

ステップS4の処理で、文書処理部22は、配布されたPDFファイル26に基づいて文書の読み取り、印刷などの処理（イベント）を行う。ステップS5の処理で、文書処理部22のプラグイン35では、PDFファイル26を受信すると、ユーザーの認証が自動的に起動する。ステップS6の処理で、プラグイン35は、PDFファイル25に埋め込まれた文書属性と、ユーザー認証により取得したユーザー属性と、イベントとをドキュメントセキュリティプロファイル処理部32に送信する。ステップS7の処理で、ドキュメントセキュリティプロファイル処理部32は、受信した文書属性、ユーザー属性、イベントとをDSP200に基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。ステップS8の処理で、ドキュメントセキュリティプロファイル処理部3

2は、文書に関する処理の許可、禁止、許可の場合の要件等の判断結果を文書処理部22に送信する。

【0067】

このように、PDFファイル25、26及びDSP200に基づいて、文書の読み取り、印刷などの処理を制御する情報を送受信することにより、文書のセキュリティの機密性を確保することができ、文書に関するセキュリティを統括して管理することができる。

【0068】

尚、埋め込み情報を埋め込んだPDFファイル25、26には、埋め込み情報を抽出するためのプログラム（例えば、AcrobatのPlug-inモジュール）がないと開けないように設定された情報を付加するようにしてもよい。

【0069】

次に、第8実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図10は、本発明の第8実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。尚、図10に示すシステム構成は、図9に示すシステム構成と略同様であるため、同様の構成及び手順については同符号を付して説明を省略する。以下、図11に示すシステム構成についても同様とする。図10において、ドキュメントセキュリティシステム80は、文書処理部21でPDFファイル25を作成する時に、DSP200に基づいて文書に関する処理の許可、禁止、許可の場合の要件等の判断を行うドキュメントセキュリティプロファイル処理部32を有する構成とされる。

【0070】

次に、ドキュメントセキュリティシステム80での処理手順を説明する。先ず、ステップS1の処理で、文書処理部21は、ドキュメントセキュリティプロファイル処理部32に文書属性と、ユーザー属性と、PDFファイル25とを送信する。ステップS2の処理で、ドキュメントセキュリティプロファイル処理部32は、受信した文書属性、ユーザー属性をDSP200に基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。ステップS3の処理で、ドキュメントセキュリティプロファイル処理部32は、文書に関する処理の

許可、禁止、許可の場合の要件等の判断結果をPDFファイル25に埋め込み、セキュリティプロテクトされたPDFファイル26を文書処理部21に送信する。ステップS4の処理で、文書処理部21は、受信したセキュリティプロテクトされたPDFファイル26を文書処理部22に配布する。

【0071】

ステップS5の処理で、文書処理部22は、配布されたPDFファイル26に基づいて文書の読み取り、印刷などの処理（イベント）を行う。ステップS6の処理で、文書処理部22のプラグイン35では、PDFファイル26を受信すると、ユーザーの認証が自動的に起動される。ステップS7の処理で、プラグイン35は、PDFファイル26に埋め込まれたユーザー属性、イベントに対する判断結果に基づいて処理を行う。

【0072】

このように、文書処理部22は、文書処理部21でPDFファイル25を作成する時に、DSP200に基づいて判断された判断結果と文書の読み取り、印刷などの処理を制御する情報を送受信することにより、文書のセキュリティの機密性を確保することができ、効率的に文書に関するセキュリティを統括して管理することができる。

【0073】

次に、第9実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図11は、本発明の第9実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図11において、ドキュメントセキュリティシステム800は、文書処理部21でPDFファイル25を作成する時に、そのPDFファイル25にDSP200を埋め込み、DSP200に基づいて文書に関する処理の許可、禁止、許可の場合の要件等の判断を行うプラグイン35を有する構成とされる。

【0074】

次に、ドキュメントセキュリティシステム800での処理手順を説明する。まず、ステップS1の処理で、文書処理部21は、ドキュメントセキュリティプロファイル処理部32に文書属性と、PDFファイル25とを送信する。ステップ

S2の処理で、ドキュメントセキュリティプロファイル処理部32は、文書情報をPDFファイル25に埋め込み、セキュリティプロテクトされたPDFファイル26を文書処理部21に送信する。ステップS3の処理で、文書処理部21は、受信したセキュリティプロテクトされたPDFファイル26を文書処理部22に配布する。

【0075】

ステップS4の処理で、文書処理部22は、配布されたPDFファイル26に基づいて文書の読み取り、印刷などの処理（イベント）を行う。ステップS5の処理で、文書処理部22のプラグイン35では、PDFファイル26を受信すると、ユーザーの認証が自動的に起動する。ステップS6の処理で、プラグイン35は、PDFファイル25に埋め込まれた文書属性、ユーザー属性、イベントとDSP200とに基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。ステップS7の処理で、プラグイン35は、受信した文書属性、ユーザー属性、イベントとをDSP200に基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。

【0076】

このように、プラグイン35がPDFファイル25、26に埋め込まれたDSP200に基づいて、文書の読み取り、印刷などの処理を制御する情報を送受信することにより、文書のセキュリティの機密性を確保することができ、文書に関するセキュリティを統括して管理することができる。

【0077】

次に、DSP200を記述するためのセキュリティポリシーについて説明する。図12は、ドキュメントに対するセキュリティポリシーの例を示す図である。図12に示すセキュリティポリシー201は、上記入出力装置10で取り扱うドキュメントに対して、入出力装置10の管理者により設定されるものとする。セキュリティポリシー201には、極秘文書についての記述202と、丸秘文書についての記述203と、社外秘文書についての記述204と、人事関連文書についての記述205とが記述されている。各記述202～205には、各ドキュメントの複写の許可の要件と、プリントの許可の要件と、閲覧の許可の要件が設定

○

されている。各記述202～205に従ってドキュメントのセキュリティレベルを分類した定義ファイルに基づいてドキュメントセキュリティポリシー200を記述する。

【0078】

次に、DSP200の先頭に記述される識別情報について説明する。図13は、DSPの識別情報を示す図である。図13に示すDSP200の識別情報210において、<about_this_policy>と</about_this_policy>とで囲まれた範囲の記述211～213には、DSP200を識別するための識別情報が記述されている。記述211には、DSP200を他のDSPと区別するためのシリアル番号が記述されている。記述212には、DSP200に対応する定義ファイルのシリアル番号が記述されている。尚、この定義ファイルは更新される可能性があるため、このDSP200がどの定義ファイルに基づいて記述されているのかを明確にするために、記述212が記述される。記述213には、DSP200のタイトル、バージョン番号、作成日時、作成者、説明などの一般的な書誌情報が記述される。

【0079】

以下に、DSP200の識別情報の後に記述される記述内容について説明する。図14は、DSPの記述例を示す図である。図14に示すDSP200の記述220において、<policy>と</policy>とで囲まれた範囲の記述221～231には、ドキュメントに関する情報が記述されている。記述220は、記述221に示す複数のアクセス制御ルール<ace_rule>で構成される。1つの記述221のアクセス制御ルール<ace_rule>は、記述222に示す対象のドキュメントのカテゴリ<doc_category>とレベル<doc_security_level>とが一意に設定され、記述223に示すアクセス制御リスト<acl>を1つ含むように設定される。記述223のアクセス制御リスト<acl>は、記述224に示す複数のアクセス制御エレメント<ace>で構成される。記述224のアクセス制御エレメント<ace>は、記述225に示すユーザーのカテゴリ<user_category>と、記述226に示すユーザーのレベル<user_security_level>とがセキュリティ属性として一意に設定される。さらに、記述224のアクセス制御エレメント<ace>

>は、記述227に示す複数のオペレーション<operation>で構成される。

【0080】

記述225に示すユーザーのカテゴリ<user_category>には、ユーザーに関するカテゴリが記述されている。また、記述226に示すユーザーのレベル<user_security_level>には、ユーザーに対してドキュメントのオペレーションが可能か否かを示す権限レベルが記述されている。尚、ユーザーのセキュリティ属性であるカテゴリとレベルの組み合わせを複数設定可能にすることにより、例えば、所定のユーザーが部門Aの「丸秘」のドキュメントとプロジェクトBの「極秘」のドキュメントの両方にアクセスすることができる。従って、ユーザーのセキュリティ属性を設けることにより、効率的にドキュメントのオペレーションを行うことができる。

【0081】

記述227の各オペレーション<operation>には、記述228に示す1つのオペレーション名<name>と、記述229に示す1つの禁止<denied/>と、記述230に示す複数の<requirement>と、記述231に示す1つの許可<allowed>などで構成される。また、図14に示すように、記述222のドキュメントのカテゴリ<doc_category>や、記述226に示すユーザーのレベル<user_security_level>に記述される「ANY」は、どのカテゴリ、レベルにも適用されることを示している。また、記述225のユーザーのカテゴリ<user_category>の「DOC_CATEGORY」はユーザーのカテゴリがドキュメントのカテゴリと同じ場合に適用される。

【0082】

このような構成でDSP200を記述することにより、ドキュメントのタイプ（カテゴリ、レベル）に応じて、どのようなユーザータイプ（カテゴリ、レベル）がドキュメントに対してどのようなオペレーションが可能なのか、オペレーションが可能な場合にはどのような要件を満たさなければならないのかを明確に記述することができる。

【0083】

また、上記DSP200は、プラットホームに依存しないXML（eXten

sible Markup Language) 形式で記述することにより、各入出力装置間でのセキュリティポリシーを共有させることができる。

【0084】

尚、セキュリティポリシーを適応させる対象は、電子的なドキュメントに限らず、上記の記述227のオペレーション<operation>に紙のドキュメントに関するオペレーション(hardcopy、scanなど)を設定することにより、紙のドキュメントに対してセキュリティポリシーを適応させることができる。

【0085】

尚、上記の記述220では、禁止するオペレーションには記述229に示すように禁止<denied/>を記述しているが、DSP200に記述されていなければアクセスは許可されていないことを表わすようにしてもよい。

【0086】

以下に、DSP200の識別情報の後に記述される記述内容の他の例について説明する。図15は、DSPの記述例を示す図である。図15に示すDSP200の記述240において、<policy>と</policy>とで囲まれた範囲のうち記述241～243には、ドキュメントのオペレーション許可に関する情報が記述されている。記述241は、<denied_operations>により許可しないオペレーションを列挙している。記述242に示す<requirement>explicit_authorization</requirement>は、ドキュメントの管理者により明示的な許可が得られた場合に、そのオペレーションを許可する記述である。記述243は、<allowed_operations>により無条件で許可するオペレーションを列挙している。

【0087】

このように、DSP200にオペレーションを明示的に許可する記述を設けることで、柔軟なオペレーション制御を行うことが可能となる。また、明示的な許可を指定可能にすることで、明示的な許可が得られれば実行可能なオペレーションと、明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができる。

【0088】

また、DSP200にオペレーション許可に関する情報を記述しないか、又は

禁止<denied/>で指定されたオペレーションは、明示的な許可が得られたとしても禁止しなければならないオペレーションとなる。これにより、ポリシーを記述している管理者側の意図が的確に設定することができ、誤って許可を与えてしまったオペレーションが実行されるというような事態を予め防ぐように設定することができる。

【0089】

次に、DSP200を記述し、管理するシステム構成について説明する。図16は、ドキュメントセキュリティポリシーの記述に関するシステム構成図である。図16において、ドキュメントセキュリティプロファイル方法において用いられるDSP200を記述し、管理するセキュリティ管理システム100は、DSPの記述、記録媒体102への格納、DSPを以下に示すサブシステムへ伝送するセキュリティサーバー101と、入出力装置10とで構成される。複数のプリンタ40、複合機50のそれぞれが入出力装置10として、ネットワーク1を介してセキュリティサーバー101に接続される。図16において、セキュリティサーバー20はサーバコンピュータであって、CPU（中央処理装置）によって各構成が制御される。CPUは、メモリユニットに格納されたプログラムに従つてセキュリティポリシー記述処理を行う。

【0090】

以下に、セキュリティ管理システム100でのDSPに関する処理を説明する。セキュリティサーバー101では、セキュリティサーバー101の管理者によりDSP200が記述される（ステップS1）。例えば、DSP200は、プラットホームに依存しないXML形式で記述される。セキュリティサーバー20は、記述されたDSP200をHDD（Hard Disk Drive）、FD（Floppy（登録商標）Disk Controller）、MO（Magnet Optical）、CD-ROM（Compact Disc Read-Only Memory）等の記録媒体102へ格納する（ステップS2）。また、セキュリティサーバー101は、ネットワーク1を介してDSP200をプリンタ40、複合機50の入出力装置10へ伝送する。

【0091】

(1)

従って、DSP200が格納された記録媒体102を各入出力装置10に配布し、また、ネットワーク1を介してDSP200を伝送することにより一貫したDSP200を各入出力装置10に反映させることができる。

【0092】

尚、セキュリティサーバー101では、DSP200をディスプレイ等の表示ユニットに表示することにより、DSP200の記述及び設定変更が行われる。また、セキュリティサーバー101が有する補助記憶装置等にDSP200を格納するようにしてもよい。

【0093】

尚、記録媒体102は、上記記録媒体に限定されることなく、DSP200を記録することができ、コンピュータが読み取り可能な媒体であれば適応可能である。

【0094】

尚、上記複合機50のかわりにコピー機を用いるようにしてもよい。

【0095】

このように、上記ドキュメントセキュリティプロファイル方法において、プリンタ40から受信した文書のセキュリティに関する文書属性情報に基づいて、文書のコンテンツに埋め込まれる埋め込み情報をプリンタ40に送信し、複合機50から受信した埋め込み情報に基づいて、文書属性情報を複合機50に送信することにより、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができる。

【0096】

また、文書を識別する文書IDに対応付けて文書属性情報と埋め込み情報を文書情報として管理する文書情報DB31を有することにより、効率的に文書のセキュリティに関する情報を参照してプリンタ40や複合機50への送受信を行うことができる。

【0097】

また、埋め込み情報が文書を一意に識別するバーコード情報、透かし情報、地

紋情報のうち少なくとも一つの情報であることにより、埋め込み情報で文書のコンテンツや文書属性を識別して文書に関する処理が実行されるため、文書のセキュリティを確保することができる。

【0098】

【発明の効果】

上述の如く本発明によれば、第1の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、文書のコンテンツに埋め込まれる埋め込み情報を第1の入出力装置に送信し、第2の入出力装置から受信した埋め込み情報をに基づいて、文書属性情報を第2の入出力装置に送信することにより、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができる。

【図面の簡単な説明】

【図1】

本発明の第1実施例に係る入出力装置のハードウェア構成を示すブロック図である。

【図2】

本発明の第1実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図3】

本発明の第2実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図4】

文書情報DBに格納されたテーブルを示す図である。

【図5】

本発明の第3実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図6】

本発明の第4実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図7】

本発明の第5実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図8】

本発明の第6実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図9】

本発明の第7実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図10】

本発明の第8実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図11】

本発明の第9実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図12】

ドキュメントに関するセキュリティポリシーの例を示す図である。

【図13】

DSPの識別情報を示す図である。

【図14】

DSPの記述例を示す図である。

【図15】

DSPの記述例を示す図である。

【図16】

ドキュメントセキュリティポリシーの記述方法におけるシステム構成図である。

。

【符号の説明】

1 ネットワーク

2～8、80、800 ドキュメントセキュリティシステム

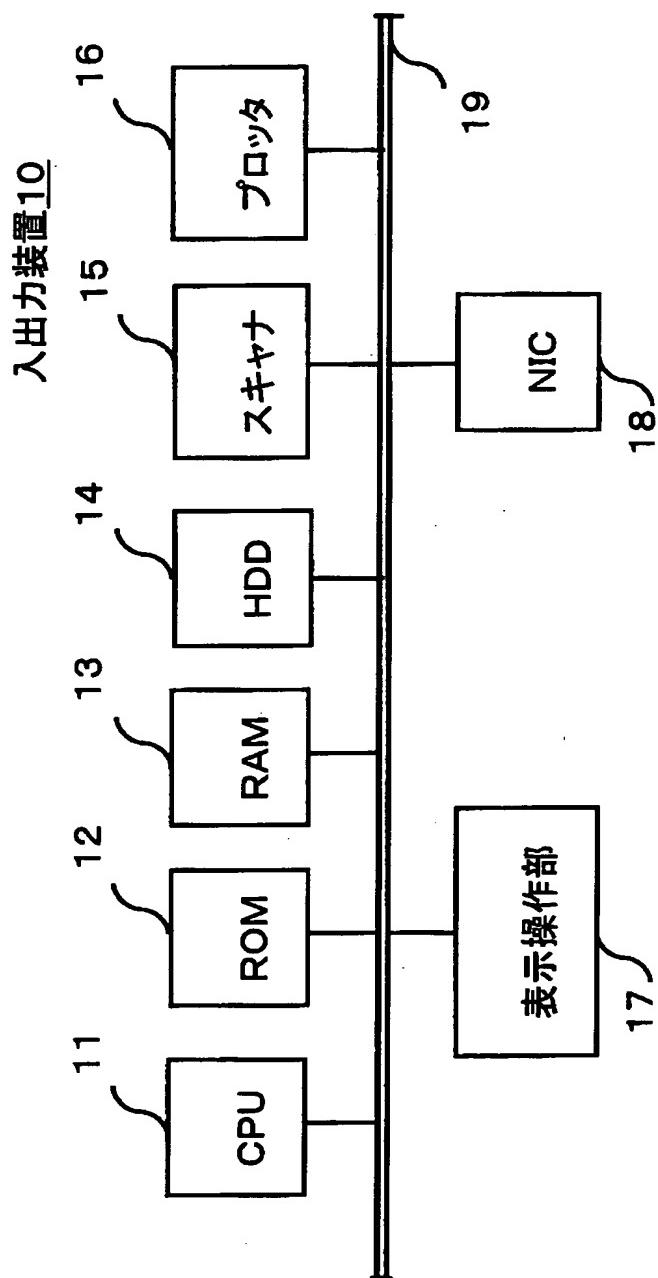
1 0	入出力装置
1 1	C P U
1 2	R O M
1 3	R A M
1 4	H D D
1 5	スキャナ
1 6	プロッタ
1 7	表示操作部
1 8	N I C
1 9	バス
2 0、2 1、2 2	文書処理部
2 5、2 6	P D F ファイル
3 0、3 2	ドキュメントセキュリティプロファイル処理部
3 1	文書情報D B
3 5	プラグイン
4 0	プリンタ
5 0、5 1	複合機
6 0	紙
6 1	埋め込み情報
7 0、7 1	アダプタ
1 0 0	セキュリティ管理システム
1 0 1	セキュリティサーバー
1 0 2	記録媒体
2 0 0	ドキュメントセキュリティポリシー

【書類名】

図面

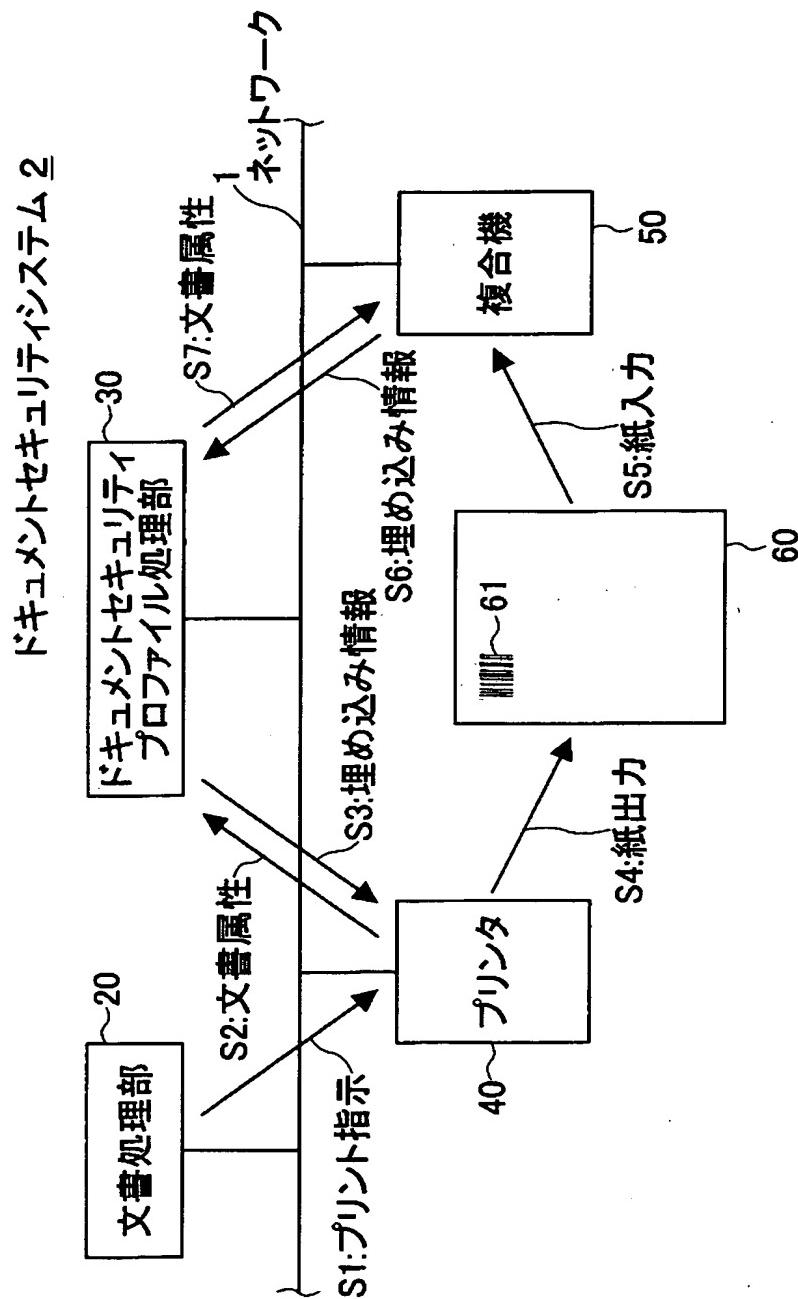
【図1】

本発明の第1実施例に係る入出力装置の
ハードウェア構成を示すブロック図



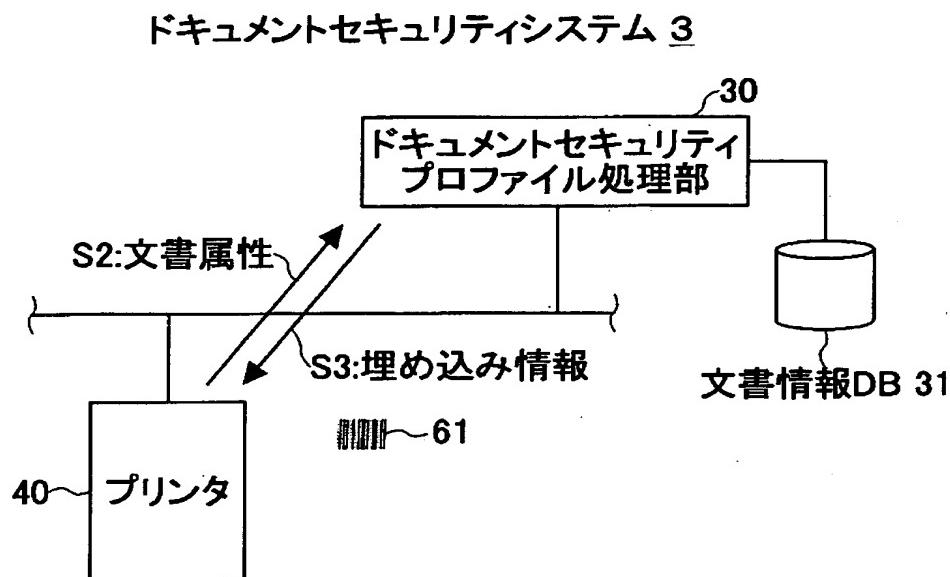
【図2】

本発明の第1実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図



【図3】

本発明の第2実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図



【図4】

文書情報DBに格納されたテーブルを示す図

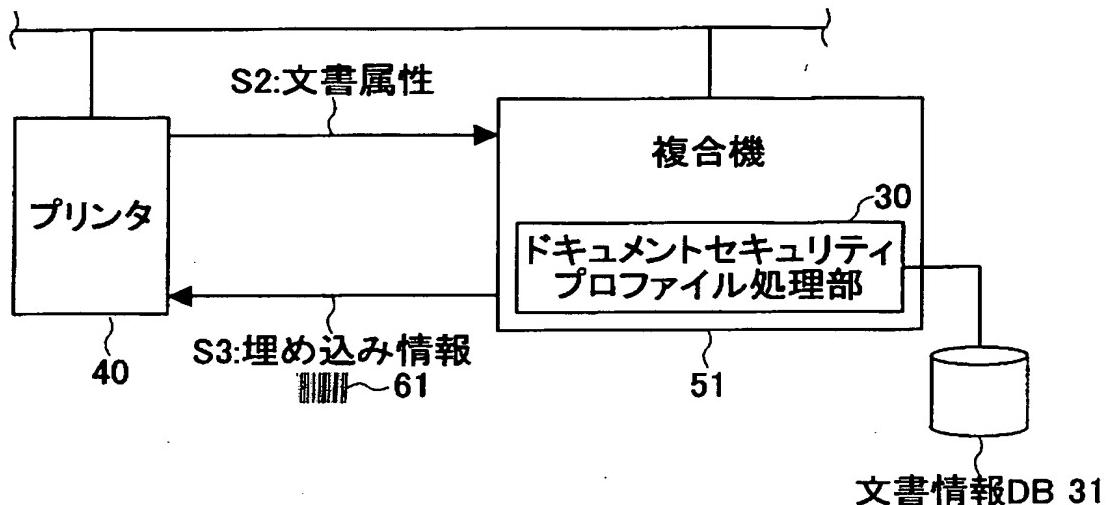
310

文書ID	文書属性ファイル	埋め込み情報
0238-20020730-1001	Attribute-23981.txt	Bar01010.bmp
0238-20020730-1002	Attribute-98263.txt	Bar01020.bmp
0238-20020730-1003	Attribute-37482.txt	Bar01030.bmp
0238-20020730-1004	Attribute-38471.txt	Bar01040.bmp

【図5】

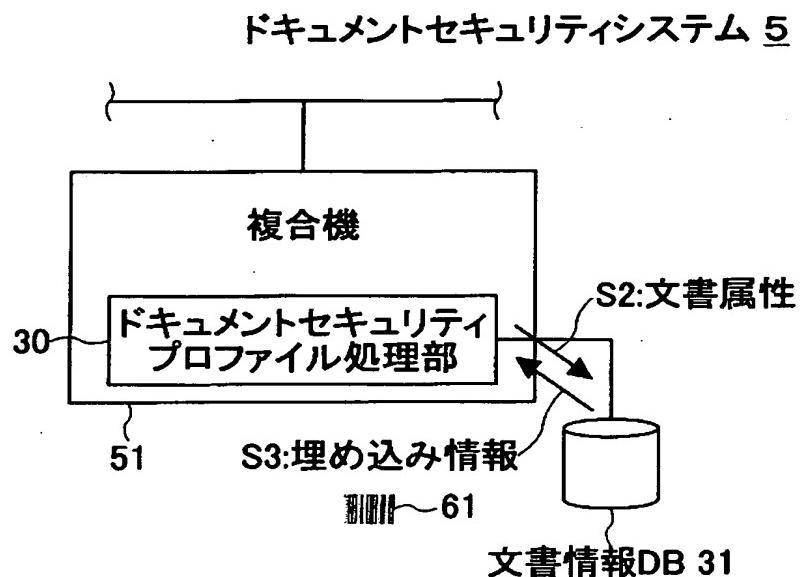
本発明の第3実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図

ドキュメントセキュリティシステム 4



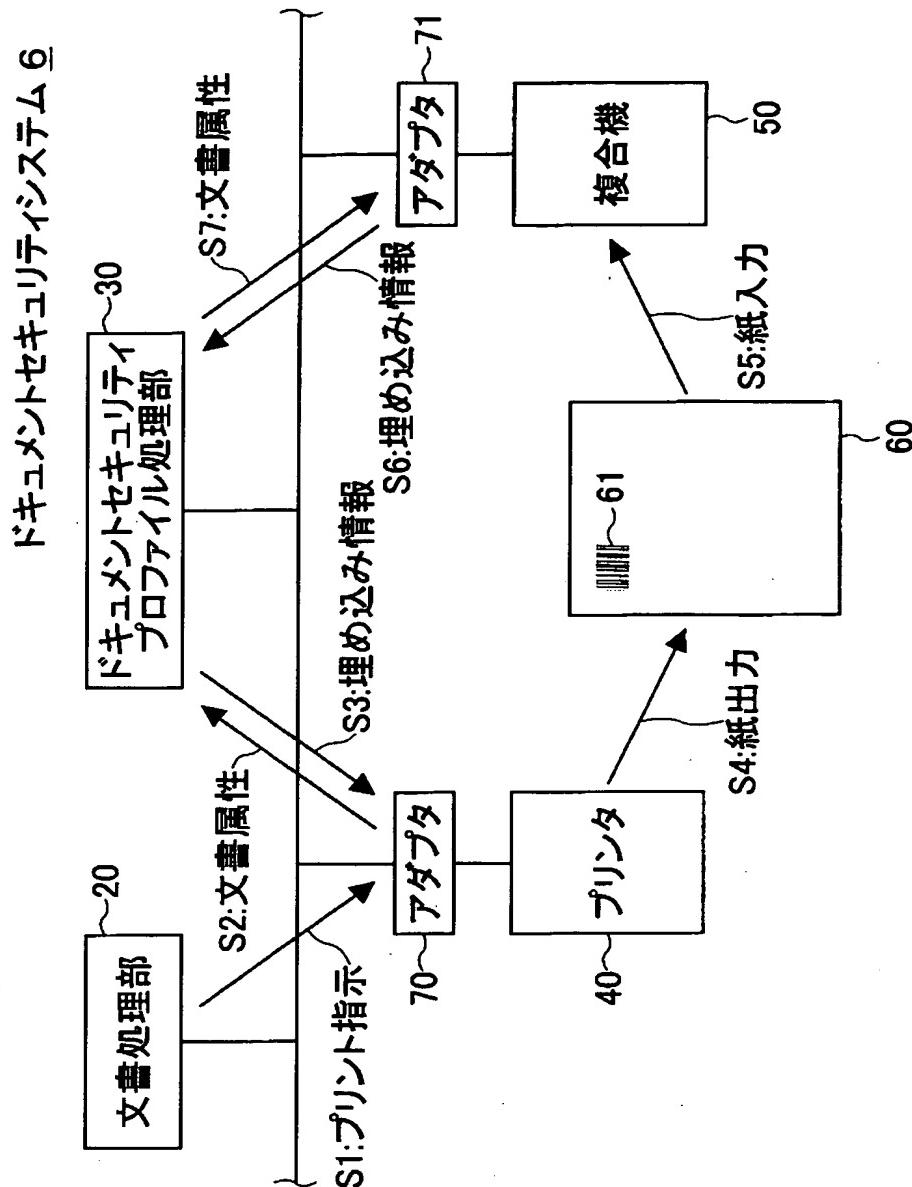
【図6】

本発明の第4実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図



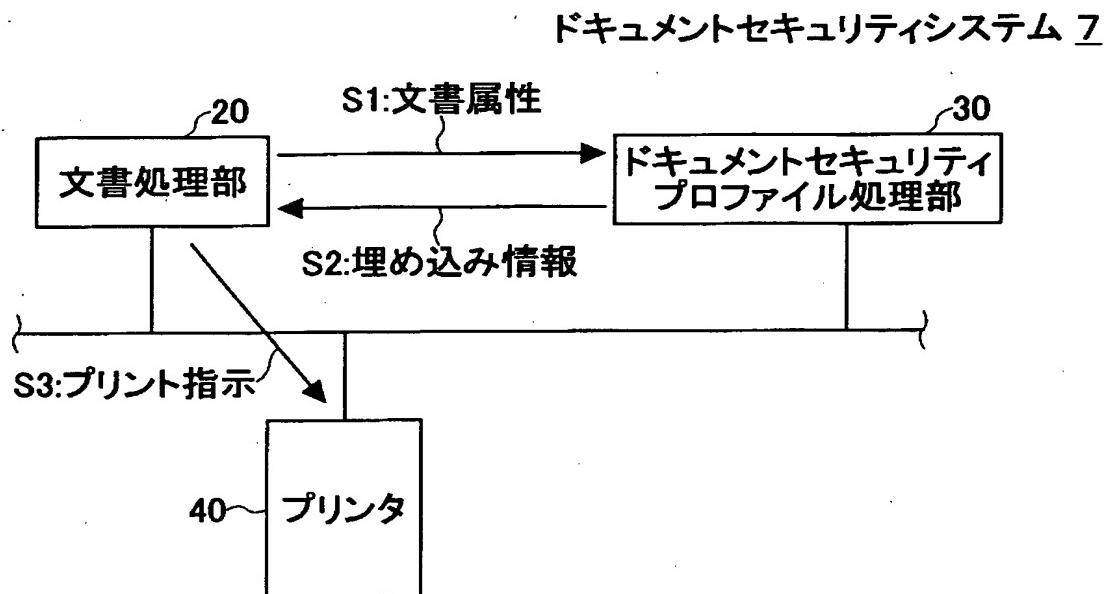
【図 7】

本発明の第5実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図



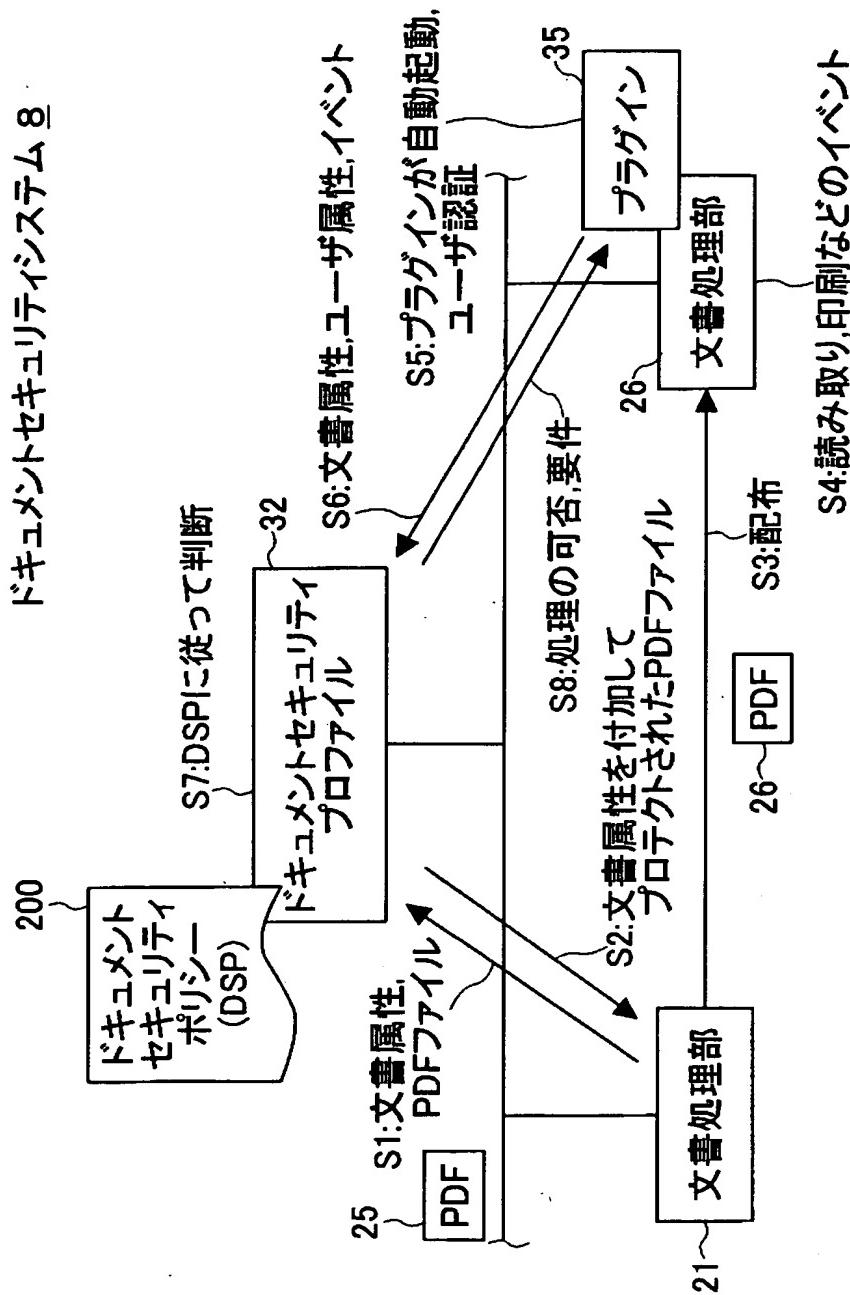
【図8】

本発明の第6実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図



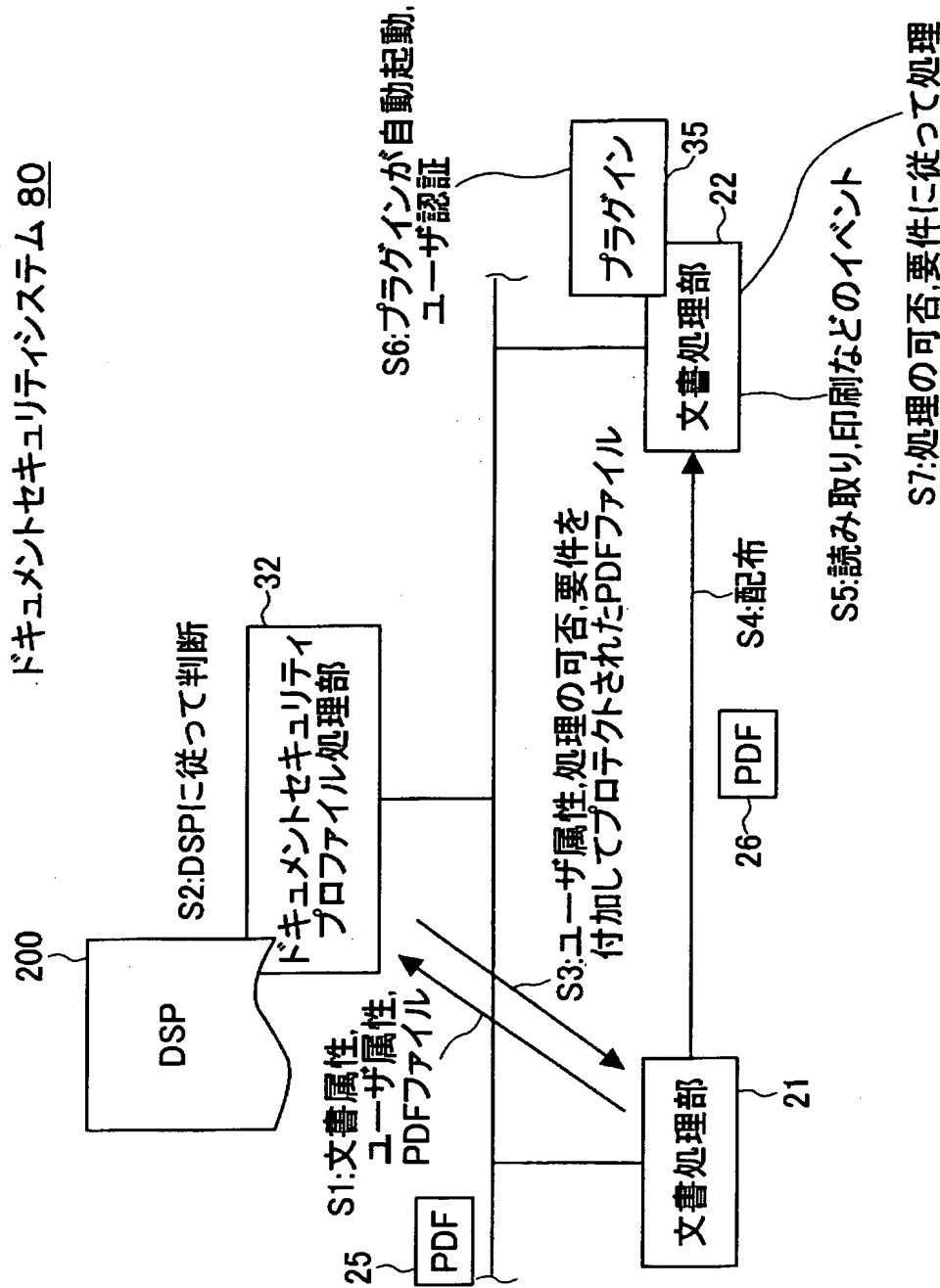
【図9】

本発明の第7実施例に係るドキュメントセキュリティ プロファイル方法におけるシステム構成図



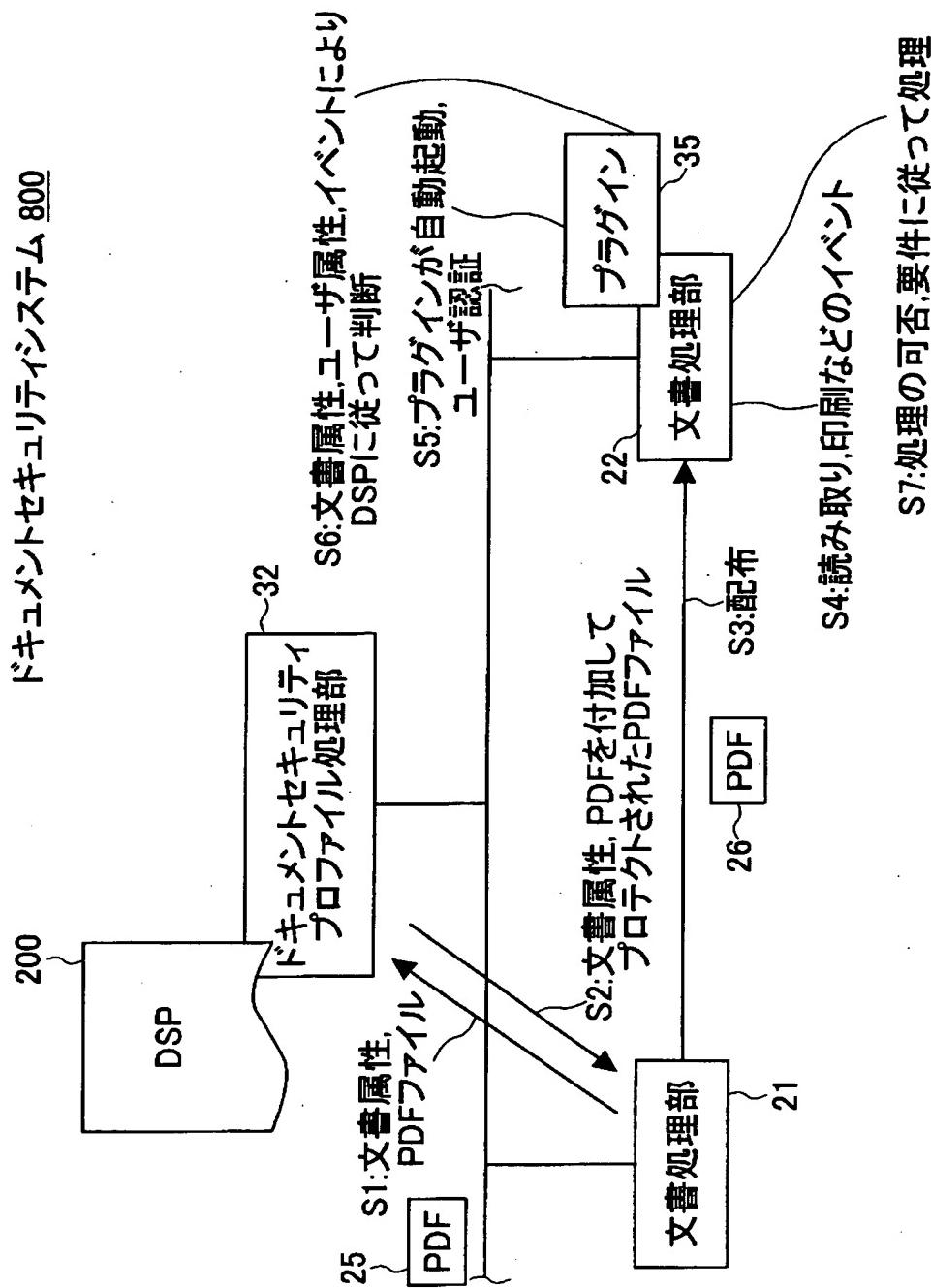
【圖 10】

本発明の第8実施例に係るドキュメントセキュリティ プロファイル方法におけるシステム構成図



【図11】

本発明の第9実施例に係るドキュメントセキュリティ
プロファイル方法におけるシステム構成図



【図12】

ドキュメントに関するセキュリティポリシーの例を示す図

201

極秘文書について：
 原則複写禁止（複写する際には管理責任者の許可を得なければならない）、
 また、複写したことを記録しておかなければならぬ、
 プリントする際には複写禁止であることを示す透かしを入れなければならぬ、
 また、プリントしたことを記録しておかなければならぬ、
 閲覧は関係者のみ許可

202～

丸秘文書について：
 複写は関係者のみ許可
 プリントする際には丸秘文書であることを示すラベルを同時に印刷しなければならぬ、
 閲覧は関係者のみ許可

203～

社外秘文書について：
 社外へ送付する際には管理責任者の許可を得なければならない、
 複写・プリント・閲覧は社内であれば許可不要

204～

人事関連文書について：
 すべて丸秘文書として取り扱う

205～

【図 13】

DSPの識別情報を示す図

210

```
<about_this_policy>
  211  <serial_number>RDSP0100-00000000000012-2023</serial_number>
  212  <terminology_applied>RDST0100-000000000001-9487</terminology_applied>
    <title>Office System Research and Development Center, DOCUMENT-SECURITY-POLICY</title>
    <version>1.20</version>
    213  <creation_date>2002/02/18 22:30:24</creation_date>
    <creator>Yoichi Kanai</creator>
    <description>This is a sample document security policy.</description>
</about_this_policy>
```

【図 14】

DSPの記述例を示す図

220

```

<policy>
221～<acc_rule>
  222～{ <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
  223～<acl>
    224～<ace>
      225～<user_category>DOC-CATEGORY
        </user_category>
      226～<user_security_level>ANY
        </user_security_level>
    227～<operation>
      228～<name>fax_send</name>
      229～<denied/><!-- denied even if it
          is explicitly authorized -->
    </operation>
    227～<operation>
      <name>net_delivery</name>
    230～<requirement>audit
      </requirement>
    231～<requirement>
      explicit_authorization
      </requirement>
      ...
    </operation>
    227～<operation>
      <name>fax_receive</name>
    231～<allowed/><!-- allowed
          without requirements -->
    </operation>
    ...
  </ace>
  224～<ace>
    ...
  </ace>
</acl>
</acc_rule>
221～<acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>high</doc_security_level>
  <acl>
    ...
  </acl>
</acc_rule>
</policy>

```

【図 15】

DSPの記述例を示す図

240

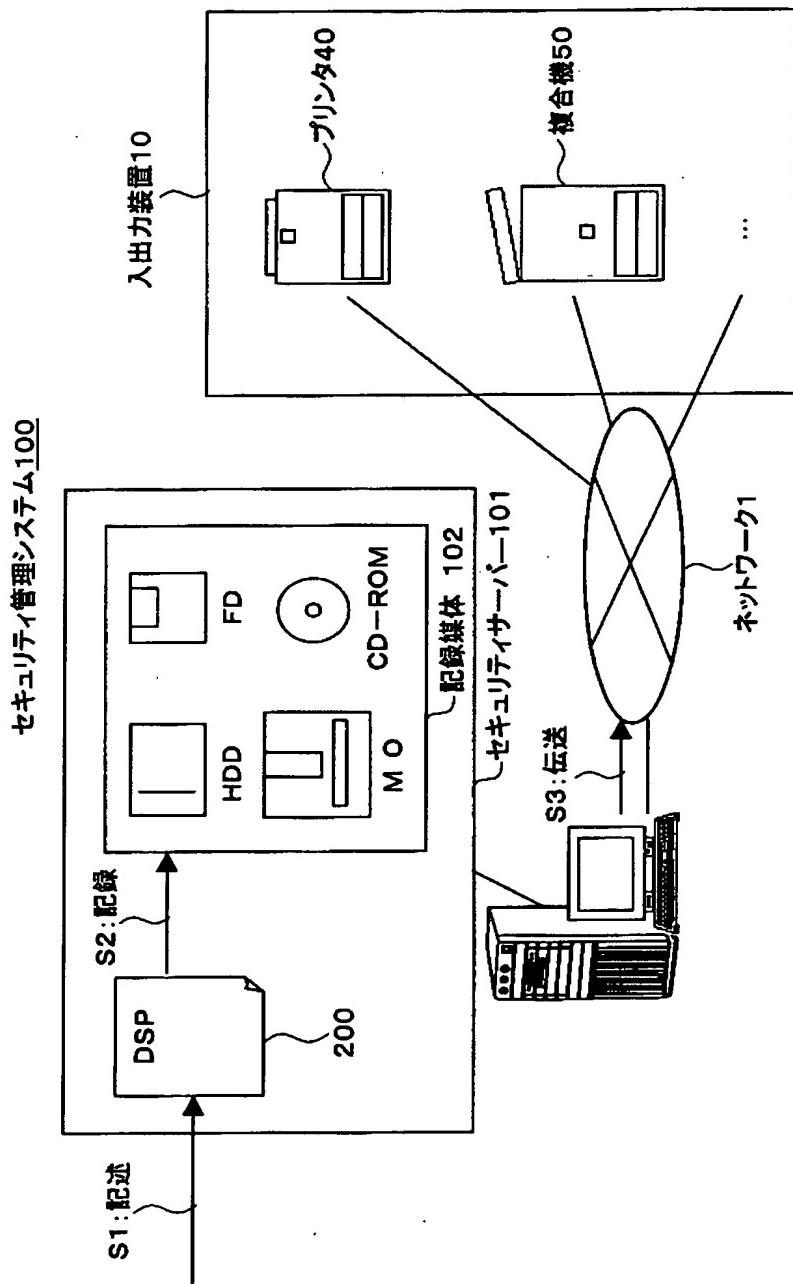
```

<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        241～<denied_operations> <!-- denied even if it is explicitly
                                     authorized -->
          <name>fax_send</name>
        </denied_operations>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
        242～<requirement>explicit_authorization
          </requirement>
          ...
        </operation>
        <operation>
          ...
        </operation>
        243～<allowed_operations> <!-- allowed without
                                     requirements -->
          <name>fax_receive</name>
          <name>store</name>
          ...
        </allowed_operations>
      </ace>
      <ace>
        ...
      </ace>
      ...
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      ...
    </acl>
  </acc_rule>
</policy>

```

【図16】

ドキュメントセキュリティポリシーの
記述方法におけるシステム構成図



【書類名】 要約書

【要約】

【課題】 文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができるドキュメントセキュリティプロファイル方法を提供することを目的とする。

【解決手段】 本発明の課題は、入出力装置との文書のセキュリティに関する情報の送受信を制御するドキュメントセキュリティプロファイル方法であって、第1の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、上記文書のコンテンツに埋め込まれる埋め込み情報を上記第1の入出力装置に送信する第1送受信手順と、第2の入出力装置から受信した上記埋め込み情報をに基づいて、上記文書属性情報を上記第2の入出力装置に送信する第2送受信手順とを有する構成とされる。

【選択図】 図2

特願2002-341222

出願人履歴情報

識別番号 [000006747]

1. 変更年月日 1990年 8月24日
[変更理由] 新規登録
住 所 東京都大田区中馬込1丁目3番6号
氏 名 株式会社リコー

2. 変更年月日 2002年 5月17日
[変更理由] 住所変更
住 所 東京都大田区中馬込1丁目3番6号
氏 名 株式会社リコー